SECURITY SYSTEM

TECHNICAL FIELD OF THE INVENTION

This invention relates to computer systems, and in particular to the improvement of security in such systems. More specifically, the invention relates to a method for improving the security of communications, for example over a computer network, although it is also applicable to increasing the security of a computer system.

BACKGROUND OF THE INVENTION

US-5,689,565 describes a cryptography system architecture for a computer, which provides cryptographic functionality to support an application which requires cryptography. The cryptography system has a cryptographic application program interface (CAPI) which interfaces with the application to receive requests for cryptographic functions. The system further includes at least one cryptographic service provider (CSP) that is independent from, but dynamically accessible by, the CAPI. The CSP provides the cryptographic functionality and manages the secret cryptographic keys.

This system architecture is used in many applications in which data may desirably be transferred across unsecured computer networks such as the internet. For example, this architecture can be used in applications such as email clients, web browsers, etc. A similar architecture can be used for access control within a computer system, and for hard disc encryption.

US-6,038,551 describes a development of the architecture disclosed in US-5,689,565, in which the computer includes a card reader, and an integrated circuit card (IC card) stores the cryptographic keys used by the CSP in the computer, and can perform

cryptographic functions in support of the CSP.

However, this system requires a user to have an IC card reader, while there is also a cost associated with the distribution of the IC cards themselves.

SUMMARY OF THE INVENTION

According to a first aspect of the present invention, a mobile communications device, having a cryptographic module, is used as a cryptographic service provider.

This has the advantage that the existing cryptographic module within the mobile communications device can be reused, thus avoiding the need to distribute additional devices.

Preferably, the mobile communications device is a WAP-enabled device, and the cryptographic module of the device is that used in WTLS.

In a preferred embodiment of the invention, a communications device which has a cryptographic module for use in mobile communications, can be used as a cryptographic services provider. For example, the device may be a device which can operate under the Wireless Application Protocol, that is, a WAP-enabled device, such as a mobile phone. This has the advantage that WAP-enabled devices include components which are used in cryptographic systems, for example public key/private key cryptographic systems, as a part of their standard communication functions. These components therefore advantageously allow the device to be used as a cryptographic services provider. Advantageously, the device can use Wireless Transport Layer Security (WTLS) for mobile communications, and employs its cryptographic module when in use as a cryptographic services provider.

It should be emphasised that the term "comprises/comprising" when used in this specification

is taken to specify the presence of stated features, integers, steps or components but does not preclude the presence or addition of one or more other features, integers, steps, components or groups thereof.

BRIEF DESCRIPTION OF DRAWINGS

Figure 1 is a block schematic diagram of a first system implementing the present invention.

Figure 2 is a flow chart showing the operation of the system of Figure 1.

Figure 3 is a flow chart showing in more detail a part of the operation illustrated in Figure 2.

Figure 4 is a block schematic diagram of a second system implementing the present invention.

Figure 5 is a block schematic diagram of a third system implementing the present invention.

Figure 6 is a flow chart showing the operation of the system of Figure 5.

DETAILED DESCRIPTION OF PREFERRED EMBODIMENTS

Figure 1 is a block schematic diagram of a computer system, including a personal computer (PC) 10, only the relevant components of which are shown. It will be apparent that, in this embodiment of the invention, and in the other illustrated embodiments, any computer system can be used in exactly the same way as the PC 10.

The computer has a connection to an external network 12, for example through a modem (not shown). Of particular concern here is the situation where the computer 10 is connected to an unsecured network, such as the internet.

The computer 10 has various software applications which require external communication, such as an email application 14, and a web browser 16, which use Secure Socket Layer (SSL) and/or Transport Layer Security (TLS) security. In many cases, the information which

is required to be sent by these applications is confidential, for example because it is personal, or could be used for criminal purposes. For example, when a user wishes to perform an online transaction, he generally needs to transmit financial information across the internet to the web site of a third party. It is therefore preferable if such transmissions can be encrypted.

As is conventional, therefore, applications such as the email application 14 and web browser 16 can call a cryptographic application program interface (CAPI) 18, which is provided on top of the operating system (OS) 20.

As is also conventional, the cryptographic application program interface (CAPI) 18 can access one or more cryptography service providers (CSPs) 22, 24.

Different cryptography service providers (CSPs) may, for example, use different cryptographic algorithms, and may be used for different purposes.

In accordance with the present invention, some or all of the functionality of a cryptography service provider is available on a separate device, namely a mobile station (MS) 30, as described in more detail below.

The mobile station may be any communications device with a suitable cryptographic module, for example a mobile phone, a personal digital assistant (PDA) or a communicator.

In this preferred embodiment, the mobile station 30 is a WAP-enabled device, for example, a mobile phone. The mobile phone 30 communicates over a wireless interface with a network, through a WAP Gateway.

In order to provide security between the WAP-enabled client device 30 and the WAP Gateway, Wireless

Transport Layer Security (WTLS) can be used. This provides confidentiality for users, by encrypting messages which are transmitted over the wireless interface, and also provides authentication, by means of digital certificates.

In order to provide this WTLS functionality, the WAP-enabled device 30 includes a cryptographic module, which uses an embedded public key and private key on handshake for authentication, then generates symmetric session keys, which are used to encode messages before transmission and to decode received messages.

For example, the phone 30 may also include a Subscriber Identity Module - Wireless Identity Module (SIM-WIM) card 32, which is used to identify the subscriber, and can contain the cryptographic module. Alternatively, the cryptographic module can be realised in hardware or in software 34 in the phone 30, or may be provided on an external smart card. In order to access the cryptographic module, the MS 30 includes a security manager module 38. The operation of these devices will be explained further below.

In accordance with preferred embodiments of the present invention, the cryptographic module of the phone, and other features which are used to provide secure communication using the Wireless Application Protocol, also allow the phone 30 to be provide some or all of the functionality of a cryptography service provider.

In the case where the cryptographic module is embodied in hardware, the necessary information is provided on an integrated circuit in the device.

Where the Wireless Public Key Infrastructure (WPKI) is used to distribute the parameters for WTLS, it can also be used to distribute the parameters required for use as a cryptography service provider.

In order to allow the PC 10 to use the mobile phone 30 as a CSP, there must obviously be a communication link between them. The connection may be wired, or wireless. Advantageously, communications between the personal computer 10 and mobile phone 30 can take place using the Bluetooth short-range radio transmission protocol, although an infrared connection is also possible. The protocol for the connection can for example be based on AT commands, and provides security for those communications. The command set is advantageously a version of the command set defined in a standard such as PKCS#11, described in the document "PKCS#11 v2.10: Cryptographic Token Interface Standard", published by RSA Security Inc. and incorporated herein by reference, where the commands are redefined as AT commands.

The PC therefore includes a modified cryptography service provider (CSP*) 26 which enables some or all of the required cryptographic functionality to be provided in the mobile phone 30. For example, the SIM-WIM card may contain the algorithm required to perform the well-known RSA encryption, but may not have sufficient memory or processing capability to calculate a message hash using the SHA-1 algorithm. In that case, the SHA-1 algorithm functionality can be provided on the modified cryptography service provider (CSP*) 26, while the RSA algorithm functionality can be provided on the MS 30.

The structure and function of the SIM-WIM card can be as defined in the document Wireless Application Protocol Identity Module Specification WAP-198-WIM, published 18 February 2000, which is incorporated by reference herein.

It will be appreciated that many other divisions of the functionality between the cryptography service

provider and the MS are possible.

Figure 2 is a flow chart showing a method by which the PC 10 can use the cryptographic functionality in the mobile phone 30.

The procedure starts with step 100, in which the application in the PC 10, such as the email application 14 or web browser 16 determines that cryptographic functionality is required, and sends a command to the CAPI 18. The cryptographic functionality which is required may for example be encryption, decryption, hash generation, message signing, verification, key generation, certificate management, or random number generation. Other types of cryptographic functionality which may be provided are described in the PKCS#11 standard mentioned above.

In step 102, the CAPI selects an appropriate CSP to provide the cryptography function. In this case, the CAPI selects the CSP* 26, which can access the cryptographic module in the MS 30.

In step 104, the CAPI 18 establishes communication with the selected CSP* 26, and the CSP* 26 establishes communications with the MS 30. As discussed above, the communications between the PC 10 and MS 30 can advantageously be over a Bluetooth short range radio link.

In step 106, the operating system (OS) 20 verifies the authenticity of the CSP*. It will be noted that this step may be unnecessary if the authenticity of the CSP* has already been established as part of an earlier process. As an alternative, this step can be carried out earlier in the process, and other changes in the order of the illustrated steps are also possible.

In step 108, a message is passed from the CAPI 18 via the CSP* 26 to the MS 30, with details of the cryptographic operation which is required.

In step 110, the required operation is carried out in the MS 30, as will be described in more detail below.

In step 112, the result of the operation in the MS 30 is sent to the CSP* 26, and then to the CAPI 18. In step 114, the CAPI 114 then responds to the application which requested the cryptographic functionality.

Figure 3 shows the operation carried out in the MS 30, as described briefly as step 110 in Figure 2 above.

In step 130, a message is received by the security manager 38, instructing the MS 30 to carry out the required cryptographic operation.

In step 132, the security manager 38 selects the appropriate functionality in the MS 30, depending on the cryptographic operation which is required.

In step 134, the security manager 38 passes the message, specifying the selected cryptographic function, to the cryptographic module, which carries out the operation in step 136.

Then, in step 138, the result of the cryptographic operation is sent back to the PC over the previously established communication link.

Thus, communications from the PC applications such as the email application 14 and web browser 16 can be encrypted using the same cryptographic functionality as WTLS, without requiring the distribution of additional keys, since the method reuses the functionality of the WAP-enabled device.

Figure 4 is a block schematic diagram of a second computer system in accordance with the invention. In this case, the system includes a personal computer (PC) 10.

The computer has a hard disc 52, and Figure 4 shows a representative software application 50 (including the hard disc drivers) which requires

communication with the hard disc 52. Since the information which is stored on the hard disc may be confidential, the application restricts access thereto, so that only authorised persons can gain access to it.

As is conventional, therefore, the hard disc application 50 can call a cryptographic application program interface (CAPI) 18, which is provided on top of the operating system (OS) 20.

As is also conventional, the cryptographic application program interface (CAPI) 18 can access one or more cryptography service providers (CSPs) 22, 24.

Different cryptography service providers (CSPs) may, for example, use different cryptographic algorithms, and may be used for different purposes.

In accordance with the present invention, as described in more detail with reference to Figures 1-3, some or all of the functionality of a cryptography service provider is available on a separate device, namely a mobile station (MS) 30, and the CSP* 26 can call the required functionality from the MS 30.

The mobile station may be exactly as described with reference to Figures 1 and 3 above.

Figure 5 shows a further alternative system in accordance with the invention.

Again, the computer system is described with reference to a personal computer (PC) 60, but it will be apparent that any computer system can be used in exactly the same way as the PC 60.

The computer has a connection to an external network 12, for example through a modem (not shown) to an unsecured network, such as the internet.

The computer 60 has various software applications which require external communication, such as an email application 14, and a web browser 16, which use Secure Socket Layer (SSL) and/or Transport Layer Security

(TLS) security.

As is conventional, applications such as the email application 14 and web browser 16 can call a PKCS#11 interface 70, as an example of a Cryptographic Application Program Interface. The PKCS#11 interface is advantageously as defined in the standards document "PKCS#11 v2.10: Cryptographic Token Interface Standard", published by RSA Security Inc.

The PKCS#11 interface 70 can access one or more cryptographic tokens (CT) 72, 74.

Different cryptographic tokens (CTs) may, for example, use different cryptographic algorithms, and may be used for different purposes.

In accordance with the present invention, some or all of the functionality of a cryptographic token is available on a separate device, namely a mobile station (MS) 30, as described in more detail below.

The PC therefore includes a modified cryptographic token (CT*) 76 which acts as a cryptography service provider, in that it can call the cryptographic functionality in the mobile phone 30, and may also include some cryptographic functionality.

As in other embodiments of the invention, the mobile station may be any communications device with a suitable cryptographic module, for example a mobile phone, a personal digital assistant (PDA) or a communicator. The mobile station (MS) 30 shown in Figure 5 is the same as that shown in Figure 1, and will not be described further.

In order to allow the PC 60 to use the mobile phone 30 as a CSP, there is a communication link between them. As in other embodiments of the invention, the connection may be wired, or wireless. Advantageously, communications between the personal computer 60 and mobile phone 30 can take place using

the Bluetooth short-range radio transmission protocol, although an infrared connection is also possible. The protocol for the connection can for example be based on AT commands, and provides security for those communications. The command set is advantageously a version of the command set defined in a standard such as PKCS#11, described in the document "PKCS#11 v2.10: Cryptographic Token Interface Standard", published by RSA Security Inc. and incorporated herein by reference, where the commands are redefined as AT commands.

Figure 6 is a flow chart showing a method by which the PC 60 can use the cryptographic functionality in the mobile phone 30.

The procedure starts with step 160, in which the application in the PC 60, such as the email application 14 or web browser 16 determines that cryptographic functionality is required, and sends a command to the PKCS#11 interface 70. The cryptographic functionality which is required may for example be encryption, decryption, hash generation, message signing, verification, key generation, certificate management or random number generation.

In step 162, the PKCS#11 interface 70 selects an appropriate CT to provide the cryptography function. In this case, the PKCS#11 interface 70 selects the CT* 76, which can access the cryptographic module in the MS 30.

In step 164, the PKCS#11 interface 70 establishes communication between the application and the selected CT* 76, and the CT* 76 establishes communications with the MS 30. As discussed above, the communications between the PC 60 and MS 30 can advantageously be over a Bluetooth short range radio link.

In step 166, a message is passed from the PKCS#11 interface 70 to the MS 30, calling the cryptographic

operation which is required.

In step 168, the required operation is carried out in the MS 30, in the same manner as was described with reference to Figure 3.

In step 170, the result of the operation in the MS 30 is sent to the CT* 26, which then responds to the application which requested the cryptographic functionality.

There are therefore disclosed methods and systems which allow encryption of communications from a computer system, or within a computer system, which can be achieved be reusing functionality which is available in an existing mobile station.